Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

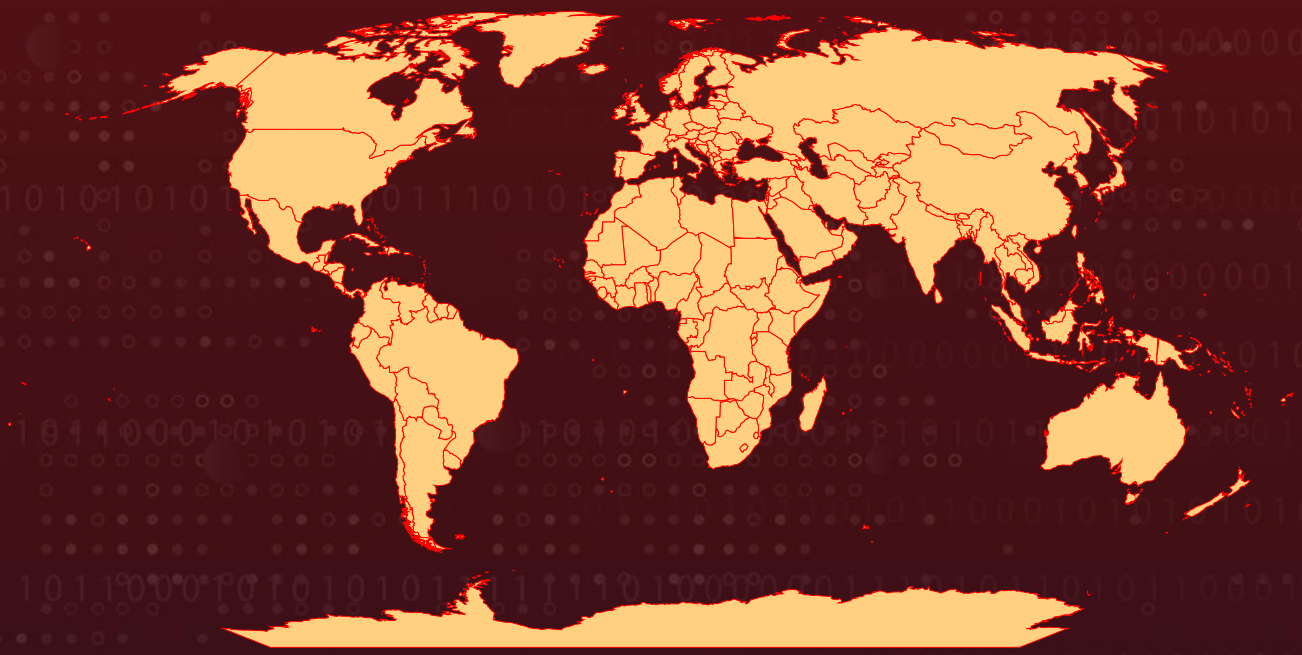
GoBruteforcer Exposed: How Weak Credentials Power a Silent Linux Botnet

Date of Publication	Admiralty Code	TA Number
January 8, 2026	A1	TA2026007

Summary

Attack Discovered: 2023
Targeted Region: Worldwide
Malware: GoBruteforcer (also called GoBrut)
Targeted Industries: Cryptocurrency
Affected Platform: Linux
Attack: GoBruteforcer is a modular Go-based botnet that compromises Linux servers by brute-forcing weak credentials on internet-exposed services such as FTP, MySQL, PostgreSQL, and phpMyAdmin, spreading through a structured infection chain that includes web shells, downloaders, IRC bots, and dedicated bruteforcer modules. The campaign is driven by the widespread reuse of AI-generated deployment examples that propagate common usernames and insecure defaults, alongside legacy web stacks like XAMPP that expose FTP and administrative interfaces with minimal hardening, leaving an estimated 50,000+ servers at risk. The operators show a clear financial motive, deploying additional Go-based tools to target cryptocurrency infrastructure, including TRON balance scanners and token-sweeping utilities for TRON and Binance Smart Chain, with on-chain analysis confirming successful theft. The 2025 variant represents a technical step forward, introducing a fully rewritten Go-based IRC bot with Garble obfuscation, process-masking for stealth, and more resilient command-and-control infrastructure.

Attack Regions



Attack Details

#1 GoBruteforcer is a steadily evolving Linux botnet written in Go that has grown far more capable since it first surfaced in 2023. Rather than relying on a single exploit, the malware follows a deliberate, multi-stage infection chain that capitalizes on weak credentials and exposed services. Initial access is typically achieved by brute-forcing FTP logins, abusing misconfigured MySQL servers, or breaking into publicly accessible phpMyAdmin panels. Systems running XAMPP are particularly attractive targets, as its default setup often exposes FTP services mapped directly to web-accessible directories, creating an easy bridge from credential access to code execution.

#2 Once attackers gain a foothold, they move quickly to establish control by uploading a PHP web shell into the compromised webroot. This web shell serves as a remote command console, allowing operators to execute arbitrary commands and prepare the system for deeper infection. From there, the attackers deploy the next stage: an IRC-based control bot. Using the web shell, architecture-specific binaries are downloaded and executed. Afterward, the bot connects back to the attacker-controlled command-and-control infrastructure over the IRC protocol, typically on TCP port 8080.

#3 The IRC bot acts as the central coordinator for further activity on the host. Through it, the attackers push down a dedicated bruteforcer module that is periodically updated and relaunched. This component continuously scans random public IP ranges, attempting credential-based logins against exposed services. The design is efficient and persistent, ensuring that compromised servers are not just victims, but active participants in expanding the botnet and harvesting new access points across the internet.

#4 The 2025 variant marks a clear technical leap. The IRC bot has been completely rewritten in Go and protected with Garble obfuscation to hinder analysis. To stay hidden, the malware masks its process name using the prctl system call, often presenting itself as the legitimate “init” process, and overwrites its command-line arguments to evade common monitoring tools. It also introduces multiple fallback command-and-control mechanisms, allowing it to recover even if primary servers are disrupted, and is compiled in multiple architecture-specific builds to maximize reach across x86, x64, and ARM-based systems.

#5 At the heart of GoBruteforcer’s success is its disciplined approach to credential abuse. Each brute-force task receives around 200 credentials from the C2 server, drawn from a larger pool of 375 to 600 commonly reused weak passwords. The malware favors predictable operational usernames such as “appuser,” “myuser,” “root,” “wordpress,” and crypto-themed variants.

#6 Millions of FTP, MySQL, and PostgreSQL servers remain publicly reachable, and researchers estimate that more than 50,000 systems are immediately vulnerable to GoBruteforcer-style attacks. Beyond simple access harvesting, the operators have demonstrated clear financial motives, especially in cryptocurrency-related campaigns. On compromised hosts, uncovered Go-based tools designed to scan TRON wallets, sweep tokens from TRON and Binance Smart Chain accounts, and automate fund transfers. In one case, data files containing around 23,000 TRON addresses were recovered, and on-chain analysis confirmed successful transfers to attacker-controlled wallets, underscoring that these attacks are not just theoretical, but actively monetized.

Recommendations

- **Audit Internet-Exposed Services:** Immediately identify and inventory all FTP, MySQL, PostgreSQL, and phpMyAdmin services exposed to the internet on your network perimeter.
- **Review Cron Jobs:** Examine all cron entries on Linux servers for suspicious persistence mechanisms executing binaries from /tmp, /var/tmp, /dev/shm, or /run/lock directories.
- **Enforce Strong Authentication:** Implement password complexity requirements (minimum 16 characters, mixed case, numbers, symbols). Deploy multi-factor authentication for all administrative interfaces. Rotate all credentials for FTP, MySQL, PostgreSQL, and phpMyAdmin services
- **Restrict Network Exposure:** Disable or firewall internet-facing FTP, MySQL, and PostgreSQL services unless absolutely required. Implement IP whitelisting for administrative interfaces. Deploy phpMyAdmin behind VPN or internal-only access
- **Monitor IRC Traffic:** Alert on outbound connections to port 8080 and unusual IRC protocol activity from internal servers.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0010 Exfiltration
TA0011 Command and Control	TA0040 Impact	T1110 Brute Force	T1110.001 Password Guessing
T1190 Exploit Public-Facing Application	T1059 Command and Scripting Interpreter	T1059.004 Unix Shell	T1059.006 Python

T1053 Scheduled Task/Job	**T1053.003** Cron	**T1505** Server Software Component	**T1505.003** Web Shell
T1027 Obfuscated Files or Information	**T1027.002** Software Packing	**T1070** Indicator Removal	**T1082** System Information Discovery
T1005 Data from Local System	**T1071** Application Layer Protocol	**T1071.001** Web Protocols	**T1095** Non-Application Layer Protocol
T1041 Exfiltration Over C2 Channel	**T1496** Resource Hijacking	**T1657** Financial Theft	**T1036** Masquerading
T1083 File and Directory Discovery	**T1046** Network Service Discovery		

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	190[.]14[.]37[.]10 93[.]113[.]25[.]114
SHA256	7423b6424b26c7a32ae2388bc23bef386c30e9a6acad2b63966188cb49c283ad, 8fd41cb9d73cb68da89b67e9c28228886b8a4a5858c12d5bb1bffb3c4addca7c, bd219811c81247ae0b6372662da28eab6135ece34716064facd501c45a3f4c0d, b0c6fe570647fdedd72c920bb40621fdb0c55ed217955557ea7c27544186aeec, ab468da7e50e6e73b04b738f636da150d75007f140e468bf75bc95e8592468e5, 4fbea12c44f56d5733494455a0426b25db9f8813992948c5fbb28f38c6367446, 64e02ffb89ae0083f4414ef8a72e6367bf813701b95e3d316e3dfbdb415562c4, c7886535973fd9911f8979355eae5f5abef29a89039c179842385cc574dfa166

TYPE	VALUE
Domains	fi[.]warmachine[.]su, xyz[.]yuzgebhmwu[.]ru, pool[.]breakfastidentity[.]ru, pandaspandas[.]pm, my.magicpandas[.]fun, pandaspandas[.]pm

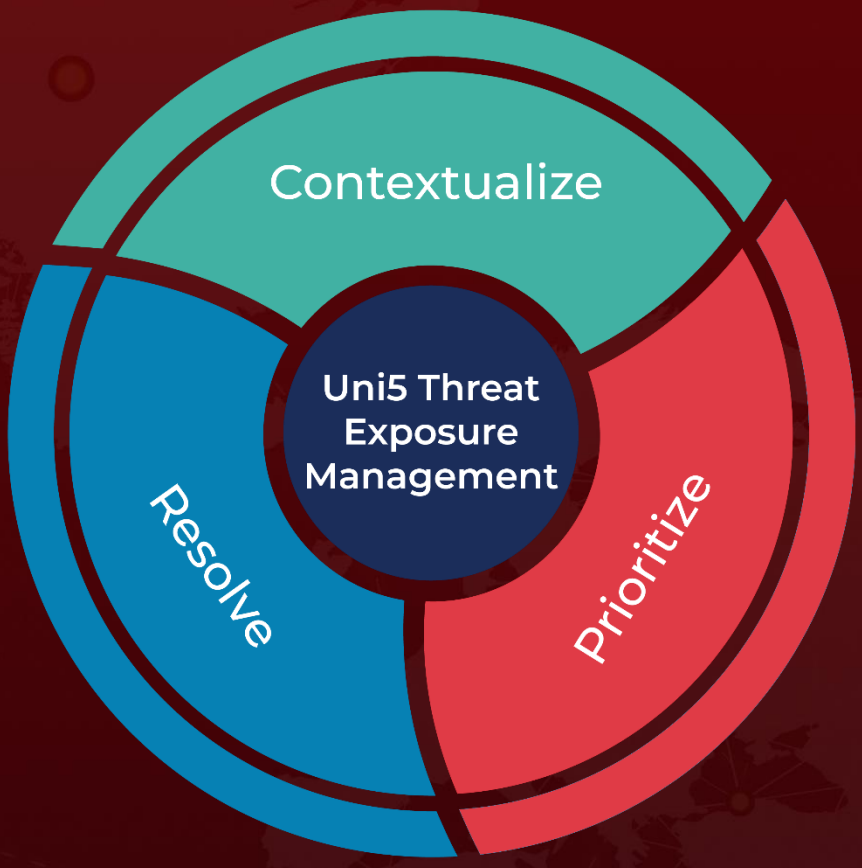
References

https://research.checkpoint.com/2026/inside-gobruteforcer-ai-generated-server-defaults-weak-passwords-and-crypto-focused-campaigns/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 8, 2026 • 11:30 PM

More at www.hivepro.com